UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,916	03/31/2004	Thomas J. Hackman	SPA07-GN002	5075

30074 7590 10/16/2008

TAFT, STETTINIUS & HOLLISTER LLP
SUITE 1800
425 WALNUT STREET
CINCINNATI, OH 45202-3957

EXAMINER	
BENOIT, ESTHER	
ART UNIT	PAPER NUMBER
2442	

MAIL DATE	DELIVERY MODE
10/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,916	HACKMAN ET AL.	
	Examiner	Art Unit	
	ESTHER BENOIT	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-73* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-73* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/6/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-73 are pending in this application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 7, 9, 18-21, 27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bilger (US 6,756,998 B1), in view of Zhao (US 6,993,501 B1).

With respect to claim 1, Bilger discloses a central system controller server operatively coupled to a data network (Col. 9, lines 51-55 and Col. 10, lines 53-61) and a residential automation computer system, operatively coupled to the data network, the residential automation computer system being associated with a residence and configured to handle one or more residential automation functions (Abstract) and the residential automation computer system being further configured to initiate a connection with the central system controller for communicating residential automation information between the central system controller and the residential automation computer system (Col. 11, lines 20-23 and lines 50-60) Bilger does not disclose the residential automation

computer system can be configured to deny all inbound data connections from the data network; however, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

With respect to claim 7, Bilger discloses the central system controller includes a plurality of central system control computers in a server farm (Col. 5, lines 63-65)

With respect to claim 9, the claim is rejection for the same reasons as claim 1 above. In addition, Zhao discloses the central system controller is configured to accept inbound connections from a remote computer operatively coupled to the data network (Col. 4, lines 31-41, where a firewall is known to have the ability to be configured to allow or deny any and all access to and from a network)

With respect to claim 18, Bilger does not disclose a firewall operatively coupled between the data network and the residential automation computer system, the firewall preventing inbound data connections to the residential automation computer system from the data network. However, Zhao discloses a firewall operatively coupled between the data network and the residential automation computer system, the firewall

preventing inbound data connections to the residential automation computer system from the data network (Col. 4, lines 31-41)

With respect to claim 19, the claim is rejected for the same reasons as claim 18 above. In addition, Zhao discloses the firewall is a hardware component separate from the residential automation computer system (Col. 4, lines 31-41)

With respect to claim 20, Bilger discloses a central system controller server operatively coupled to a data network (Col. 9, lines 51-55 and Col. 10, lines 53-61) a residential automation computer system associated with a residence and configured to handle one or more residential automation functions (Abstract). Bilger does not disclose a firewall operatively coupling the residential automation computer system to the data network and being configured to deny all inbound data connections from the data network to the residential computer. However, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

With respect to claim 21, Bilger discloses the residential automation computer system is further configured to initiate a connection with the central system controller

over the data network for communicating residential automation information between the central system controller and the residential automation computer system (Abstract).

With respect to claim 27, Bilger discloses the central system controller includes a plurality of central system control computers in a server farm (Col. 5, lines 63-65)

With respect to claim 29, the claim is rejection for the same reasons as claim 1 above. In addition, Zhao discloses the central system controller is configured to accept inbound connections from a remote computer operatively coupled to the data network (Col. 4, lines 31-41, where a firewall is known to have the ability to be configured to allow or deny any and all access to and from a network)

4. Claims 2-6, 8, 10-17, 22-26, 28, and 30-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bilger (US 6,756,998 B1), in view of Zhao (US 6,993,501 B1), and further in view of Bergstrom et al. (*Making Home Automation Communications Secure*, 2001)

With respect to claim 2, Bilger and Zhao do not disclose the connection with the central system controller is a secure connection. However, in *Making Home Automation Communications Secure*, Bergstrom discloses the connection with the central system controller is a secure connection (pg. 50, paragraph 1 and 2, “Long the futuristic…”)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger and Zhao with the

teachings of Bergstrom to make the connection with the central controller a secure connection, in order to provide security to the home automation system and prevent any unauthorized users from gaining access to it.

With respect to claim 3, the claim is rejected for the same reasons as claim 2 above. In addition, Bergstrom discloses the connection with the central system controller is a maintained secure connection (pg. 50, paragraph 1 and 2, “Long the futuristic…”)

With respect to claim 4, the claim is rejected for the same reasons as claim 3 above. In addition, Bergstrom discloses the maintained secure connection is periodically renegotiated (pg. 55,”Encryption Algorithms...”)

With respect to claim 5, the claim is rejected for the same reasons as claim 2 above. In addition, Bergstrom discloses the secure connection utilizes encryption algorithms for communications between the residential automation computer system and the central system controller (pg. 55,”Encryption Algorithms...”)

With respect to claim 6, the claim is rejected for the same reasons as claim 2 above. In addition, Bergstrom discloses the secure connection utilizes public/private key pair techniques for communications between the residential automation computer system and the central system controller (pg. 55,”Encryption Algorithms...”)

With respect to claim 8, Bilger and Zhao do not disclose the central system controller includes a plurality of central system controller computers, each central system controller computer being associated with a specific geographic region.

However, Bergstrom discloses each central system controller computer being associated with a specific geographic region (pg. 51, "Global Home Server...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger and Zhao with the teachings of Bergstrom to associate the central system controller with a specific geographic region, in order to associate the central controller with a region within the global network.

With respect to claim 10, Bilger and Zhao do not disclose the central system controller includes an authentication algorithm for controlling access to the central system controller to an authorized user of the remote computer. However, Bergstrom discloses disclose the central system controller includes an authentication algorithm for controlling access to the central system controller to an authorized user of the remote computer (pg. 55, "Encryption Algorithm…")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger and Zhao with the teachings of Bergstrom to include an authentication algorithm, in order to prevent unauthorized users from accessing the home automation system.

With respect to claim 11, the claim is rejection for the same reasons as claim 10 above. In addition, Bergstrom discloses the central system controller monitors for unauthorized access from the remote computer (pg. 55, "Encryption Algorithm…")

With respect to claim 12, the claim is rejected for the same reasons as claim 1 above. In addition, Bergstrom discloses the data network is a global computer network (pg. 51, "Global home Server…")

With respect to claim 13, the claim is rejected for the same reasons as claim 12 above. In addition, Bergstrom discloses the global computer network is the World-Wide-Web (pg. 51, "Global home Server…")

With respect to claim 14, the claim is rejected for the same reasons as claim 13 above. In addition, Bergstrom discloses the central system controller provides an access Web site on the World-Wide-Web that is configured to accept Web access from a remote computer operatively coupled to the World-Wide-Web (pg. 51, "Global home Server…")

With respect to claim 15, the claim is rejection for the same reasons as claim 10 above. In addition, Bergstrom discloses the access Web site is password protected for controlling access to the central system controller to authorized users (pg. 55, "Encryption Algorithms")

With respect to claim 16, Bilger discloses the access Web site is configured to allow an authorized user of the remote computer to communicate with the residential automation computer system, wherein communications between the remote computer and the residential automation computer system are transferred over the connection initiated with the central system controller by the residential automation computer system (Col. 11, lines 20-23 and lines 50-60)

With respect to claim 17, Bilger discloses the communications between the remote computer and the residential automation computer system are indirect communications that are processed by the central system server (Abstract)

With respect to claim 22, the claim is rejected for the same reasons as claim 5 above. Please see rejection.

With respect to claim 23, the claim is rejected for the same reasons as claim 20 above. In addition, Bergstrom discloses the maintained secure connection is periodically renegotiated (pg. 55,"Encryption Algorithms...")

With respect to claim 24, the claim is rejection for the same reasons as claim 23 above, In addition, Zhao discloses wherein the maintained secure connection on the data network is initiated by at least one of the residential automation computer system and the firewall (Col. 4, lines 31-41, where a firewall is known to have the ability to be configured to allow or deny any and all access to and from a network)

With respect to claims 25-26, the claims are rejected for the same reasons as claims 4 and 5 respectively above. Please see rejection.

With respect to claim 28, the claim is rejected for the same reasons as claim 8 above. Please see rejection.

With respect to claims 30-35, the claims are rejected for the same reasons as claims 10-15 respectively above. Please see rejection.

With respect to claim 36, Bilger does not disclose wherein the access Web site is configured to allow an authorized user of the remote computer to communicate with the residential automation computer system, wherein communications between the remote computer and the residential automation computer system are transferred over a connection initiated with the central system controller by at least one of the residential automation computer system and the firewall. However, Zhao discloses an automated system that includes a firewall that is able to be set to accept or reject inbound data connections from an outside network or authorized user (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

With respect to claim 37, Bilger discloses the communications between the remote computer and the residential automation computer system are indirect communications that are processed by the central system server (Abstract)

With respect to claim 38, Bilger does not disclose wherein the access Web site is configured to allow an authorized user of the remote computer to communicate with the residential automation computer system, wherein communications between the remote computer and the residential automation computer system are transferred over a maintained connection between the central system controller and at least one of the residential automation computer system and the firewall. However, Zhao discloses an automated system that includes a firewall that is able to be set to accept or reject

inbound data connections from an outside network or authorized user (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

5. Claims 39-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bilger (US 6,756,998 B1), in view of Zhao (US 6,993,501 B1), and further in view of Bergstrom et al. (*Making Home Automation Communications Secure*, 2001)

With respect to claim 39, Bilger discloses a central system controller server operatively coupled to a data network (Col. 9, lines 51-55 and Col. 10, lines 53-61) and a residential automation computer system, operatively coupled to the data network, the residential automation computer system being associated with a residence and configured to handle one or more residential automation functions (Abstract). Bilger does not disclose the residential automation computer system being configured to deny all inbound data connections from the data network; However, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

Bilger, in view of Zhao, does not disclose and the residential automation computer system being connected with the central system controller over the data network by a maintained secure connection. However, in *Making Home Automation Communications Secure*, Bergstrom discloses the connection with the central system controller is a secure connection (pg. 50, paragraph 1 and 2, “Long the futuristic…”)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger and Zhao with the teachings of Bergstrom to make the connection with the central controller a secure connection, in order to provide security to the home automation system and prevent any unauthorized users from gaining access to it.

With respect to claim 40, the claim is rejected for the same reasons as claim 39 above. In addition, Bergstrom discloses the maintained secure connection is initiated by the residential automation computer system (pg. 55,”Encryption Algorithms...”)

With respect to claim 41, the claim is rejected for the same reasons as claim 3 above. In addition, Bergstrom discloses the maintained secure connection is periodically renegotiated (pg. 55,”Encryption Algorithms...”)

With respect to claims 42-48, the claims are rejected for the same reasons as claims 9-15 respectively above. Please see rejection.

With respect to claim 49, the claim is rejected for the same reasons as claim 47 above. In addition, Bergstrom discloses the access Web site is configured to allow an authorized user of the remote computer to communicate with the residential automation computer system, wherein communications between the remote computer and the residential automation computer system are transferred over the maintained secure connection.

With respect to claim 50, the claims are rejected for the same reasons as claims 17 above. Please see rejection.

With respect to claim 51, Bilger discloses a central system controller server operatively coupled to a data network (Col. 9, lines 51-55 and Col. 10, lines 53-61) a residential automation computer system, operatively coupled to the data network, the residential automation computer system being associated with a residence and configured to handle one or more residential automation functions (Abstract) Bilger does not disclose means for blocking all inbound connections or connection requests to the residential automation computer system over the data network; However, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of

Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

Bilger, in view of Zhao, does not disclose means for initiating a secure connection by the residential automation computer system with the central system controller over the data network; means for accessing the central system controller by an authorized user on a remote computer; and means for facilitating communications between the authorized user on the remote computer and the residential automation computer system via the central system controller and the secure connection. However, in *Making Home Automation Communications Secure*, Bergstrom discloses the connection with the central system controller is a secure connection (pg. 50, paragraph 1 and 2, "Long the futuristic…")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger and Zhao with the teachings of Bergstrom to make the connection with the central controller a secure connection, in order to provide security to the home automation system and prevent any unauthorized users from gaining access to it.

6. Claims 52-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bergstrom et al. (*Making Home Automation Communications Secure*, 2001) , in view of Zhao (US 6,993,501 B1)

With respect to claim 52, Bergstrom discloses initiating by the residential automation computer system a secure connection with the central system controller (pg. 53, Col. 2, paragraph 1, "For layering to work…") communicating residential automation system information between the central system controller and the residential automation computer system over the secure connection (pg. 53, Col. 2, "Security layer…") Bergstrom does not disclose blocking all inbound connections to the residential automation computer system over the data network; However, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bergstrom with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

With respect to claims 53-56, the claims are rejected for the same reasons as claims 3-6, respectively above. Please see rejection.

With respect to claim 57, the claim is rejected for the same reasons as claim 21 above. Please see rejection.

With respect to claim 58-59, the claims are rejected for the same reasons as claims 10-11 respectively above. Please see rejection.

With respect to claim 60, Bergstrom discloses the data network is the World-Wide-Web (pg. 51, "Global Home Server…") the accessing step includes the steps of

providing an accessing Web site by the central system controller and logging onto the accessing Web site by the remote computer (pg. 51, "Global Home Server…") and the communication step includes the step of communicating residential automation system information between the remote computer and the residential automation computer system via the accessing Web site (pg. 51, "Global Home Server…")

With respect to claim 61, Bergstrom discloses maintaining a secure connection between the residential automation computer system and the central system controller on the data network (pg. 53, Col. 2, paragraph 1, "For layering to work…") communicating residential automation system information between the central system controller and the residential automation computer system over the secure connection (pg. 53, Col. 2, "Security layer…") Bergstrom does not disclose blocking all inbound connections to the residential automation computer system over the data network; However, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bergstrom with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

With respect to claims 62-64, the claims are rejected for the same reasons as claims 4-6 respectively above. Please see rejection.

With respect to claim 65, the claim is rejected for the same reasons as claim 21 above. Please see rejection.

With respect to claims 66-67, the claims are rejected for the same reasons as claims 10-11 respectively above. Please see rejection.

With respect to claim 68, the claim is rejected for the same reasons as claim 60 above. Please see rejection.

7. Claims 69, and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable Bilger (US 6,756,998 B1), in view of Bergstrom et al. (*Making Home Automation Communications Secure*, 2001)

With respect to claim 69, Bilger discloses accessing a central system controller by the remote computer over the data network (Col. 9, lines 51-55 and Col. 10, lines 53-61) communicating residential automation system information between the remote computer and the central system controller (Col. 11, lines 20-23 and lines 50-60) Bilger does not disclose initiating by the residential automation computer system a secure connection on the data network between the residential automation computer system and the central system controller; and communicating residential automation system information between the central system controller and the residential automation computer system over the secure connection between the central system controller and the residential automation computer system. However, in *Making Home Automation*

Communications Secure, Bergstrom discloses the connection with the central system controller is a secure connection (pg. 50, paragraph 1 and 2, "Long the futuristic…")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Bergstrom to make the connection with the central controller a secure connection, in order to provide security to the home automation system and prevent any unauthorized users from gaining access to it.

With respect to claim 71, Bilger discloses accessing a central system controller by the remote computer over the data network (Col. 9, lines 51-55 and Col. 10, lines 53-61) communicating residential automation system information between the remote computer and the central system controller (Col. 11, lines 20-23 and lines 50-60) Bilger does not disclose maintaining a secure connection on the data network between the residential automation controller and the central system controller; and communicating residential automation system information between the central system controller and the residential automation computer system over the secure connection between the central system controller and the residential automation computer system. However, in *Making Home Automation Communications Secure*, Bergstrom discloses the connection with the central system controller is a secure connection (pg. 50, paragraph 1 and 2, "Long the futuristic…")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Bergstrom to make the connection with the central controller a secure connection, in

order to provide security to the home automation system and prevent any unauthorized users from gaining access to it.

8. Claims 70, and 72-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bilger (US 6,756,998 B1), in view of Bergstrom et al. (*Making Home Automation Communications Secure*, 2001), and further in view of Zhao (US 6,993,501 B1)

With respect to claims 70 and 72, Bilger does not disclose the residential automation computer system can be configured to deny all inbound data connections from the data network; however, Zhao discloses an automated system that includes a firewall that is able to be set to reject inbound data connections from an outside network (Col. 4, lines 31-41)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bilger with the teachings of Zhao to incorporate a firewall into the home automation system, in order to prevent any unauthorized users from gaining access to the home automation network.

With respect to claim 73, the claim is rejected for the same reasons as claim 3 above. In addition, Bergstrom discloses the maintained secure connection is periodically renegotiated (pg. 55,"Encryption Algorithms...")

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esther Benoit whose telephone number is 571-270-3807. The examiner can normally be reached on Monday through Friday between 7:30 a.m and 5 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2442

E.B.
October 9, 2008